

Attorney Docket # 2132-45PCON

COPY OF PAPERS
ORIGINALLY FILED

Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Harri VATANEN

Serial No.: 09/835,668

Filed: April 16, 2001

For: Method and System for Application of a
Safety Marking



LETTER TRANSMITTING PRIORITY DOCUMENTS

Assistant Commissioner for Patents
Washington, D.C. 20231

SIR:

In order to complete the claim to priority in the above-identified application under 35 U.S.C. §119, enclosed herewith is a certified copy of each foreign application on which the claim of priority is based: Application No. FI 982232, filed on October 14, 1998, in Finland and Application No. PCT/FI99/00851, filed on October 14, 1999, in Finland.

Respectfully submitted,
COHEN, PONTANI, LIEBERMAN & PAVANE

By

Edward M. Weisz
Reg. No. 37,257
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: January 10, 2002

PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 3.4.2001

COPY OF PAPERS
ORIGINALLY FILED



ETUOIKEUSTODISTUS
PRIORITY DOCUMENT



Hakija
Applicant

Sonera Oy
Helsinki

COHEN, PONTANI, LIEBERMAN & PAVANI

Patenttihakemus nro
Patent application no

982232

APR 23 2001

Tekemispäivä
Filing date

14.10.1998

RECEIVED

Kansainvälinen luokka
International class

H04L

Keksinnön nimitys
Title of invention

"Menetelmä ja järjestelmä turvamerkinän käyttämiseksi"

Hakijan nimi on hakemusdiaariin 13.08.2000 tehdyn nimenmuutoksen jälkeen **Sonera Oyj**.

The application has according to an entry made in the register of patent applications on 13.08.2000 with the name changed into **Sonera Oyj**.

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.


Pirjo Kaila
Tutkimussihteeri

Maksu 300,- mk
Fee 300,- FIM

Osoite: Arkadiankatu 6 A Puhelin: 09 6939 500
P.O.Box 1160 Telephone: + 358 9 6939 500
FIN-00101 Helsinki, FINLAND

Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

MENETELMÄ JA JÄRJESTELMÄ TURVAMERKINNÄN KÄYTTÄMISEKSI

KEKSINNÖN ALA

5 Esillä oleva keksintö koskee elektronista turvamerkintää. Erityisesti esillä olevan keksinnön kohteena on uusi ja parannettu menetelmä ja järjestelmä sähköisessä muodossa olevan turvamerkinnän käyttämiseksi esineiden ja laitteiden merkitsemiseen.

10 TEKNIIKAN TASO

Turvamerkintää käytetään esineiden, laitteiden sekä informaation merkintään niiden suojaamiseksi varkaudelta ja väärinkäytöltä. Turvamerkintä voi olla laitteeseen kaiverrettu omistajan sosiaaliturvatusnimi tai muu tieto, joka yksilöi laitteen omistajan. 15 Tämän toteuttaminen on kuitenkin hankalaa, koska kaivertaminen tai muu vastaava fyysinen merkintätapa voi aiheuttaa merkittävälle laitteelle vaurioita ja merkintä on usein epäesteettinen.

20 Turvamerkintä voi perustua myös biometriseen tietoon, jollainen on esimerkiksi DNA, sormenjälki tai silmästä saatava tieto, jolloin henkilön identiteetti on paremmin varmistettavissa. Toisaalta esimerkiksi kloonatuilla yksilöillä DNA on identtinen, mutta sormenjälki erilainen. Tunnistuksen tarkkuutta voidaan 25 entisestään parantaa yhdistämällä erilaisia toisistaan riippumattomia tunnisteita. Ihmisen DNA voidaan muodostaa $2^{44} \approx 1,76 \cdot 10^{13}$ erilaisella tavalla. Vastaavasti maapallon väkiluvun suuruusluokka on noin 10^{10} . Yhdistämällä DNA:han siitä riippumaton sormenjälki, ja 30 esimerkiksi matkaviestimen yhteydessä esiintyvä PIN-koodi saadaan erilaisiksi kombinaatioiksi esimerkiksi 10^{29} .

35 Nykyään esineitä voidaan merkitä myös sähköisellä tai elektronisella turvamerkinnällä, jonka perusideana on merkitä esineet pienellä koodatulla tur-

vasirulla, jonka sisältämän merkintätiedon voi lukea ja tunnistaa ainoastaan erikoislukulaitteilla. Eräs tällainen järjestelmä perustuu transponderitekniikkaan, joka on liitetty lähes näkymättömiin siruihin.

5 Yleensä sirut ovat passiivisia, jolloin niitä ei voida uudelleen ohjelmoida, mikä estää niiden väärentämisen ja ne eivät myöskään näin ollen ole herkkiä sähkömagneettiselle säteilylle. Elektronista turvamerkintää käytetään siten, että asiakas ostaa turvamerkinnän

10 valtuutetulta jälleenmyyjältä. Jälleenmyyjä asentaa mikrosirun merkittävään esineeseen, minkä jälkeen rekisterikortin avulla rekisteröidään merkintä kolmannen osapuolen ylläpitämään tietokantaan.

Kun varastettu ja turvamerkitty esine löydetään, luetaan erikoislukulaitteella sirun sisältämä sähköinen informaatio. Tätä informaatiota verrataan kolmannen osapuolen tietokantaan, jolloin tietokannasta saadaan selville esineen oikea omistaja. Tällainen järjestely kuitenkin vaatii erityisen rekisteröintitietokannan, joka vaatii ylläpitoa ja on siten hankala

20 käyttää. Lisäksi lukulaitetta tai luettua informaatiota voidaan muokata tai manipuloida ennen rekisteritietokannasta tehtävää kyselyä. Tämän johdosta järjestelmään ei voi täysin luottaa.

25 Esillä olevan keksinnön tarkoituksena on poistaa edellä esitetyt ongelmat.

Erityisesti esillä olevan keksinnön tarkoituksena on tuoda esiin uudentyyppinen menetelmä ja järjestelmä esineiden, laitteiden tai informaation

30 elektronista merkintää varten. Keksinnön tarkoituksena on yksinkertaistaa merkittyjen laitteiden tunnistaminen ja aikaansaada järjestelmä, joka on ehdottoman luotettava.

Esillä oleva keksintö kohdistuu menetelmään

35 turvamerkinnän käyttämiseksi. Menetelmässä turvamerkintä liitetään sähköisessä muodossa merkittävään laitteeseen. Merkintä voidaan asentaa laitteeseen tai

esineeseen niin huomaamattomasti, että sen havaitseminen on käytännössä mahdotonta.

Keksinnön mukaisesti turvamerkintä luetaan tunnistuslaitteeseen ja avataan se siihen sisältyvien tietojen saamiseksi. Tietoihin voi kuulua henkilökoh-
 5 taiset omistajan tunnistetiedot, kuten nimi, sosiaali-
 turvatunnus ja niin edelleen. Tässä yhteydessä voidaan soveltaa myös esimerkiksi PIN-koodia (PIN, Personal Identity Number), jolloin voidaan muodostaa sähköinen
 10 allekirjoitus. Käytettävä PIN-koodi voidaan toteuttaa joko matkaviestimessä tai SIM-kortilla. PIN-koodi ja sen pituus voidaan määritellä sovellukseen sopivaksi, käyttäjä voi myös eräässä sovelluksessa vaihtaa sen
 15 niin halutessaan.

Keksinnön eräässä sovelluksessa turvamerkintä muodostetaan siten, että henkilökohtaisista tai muista identifiointitiedoista muodostetaan ensimmäinen merk-
 20 kijono, joka on ennalta määrättyssä muodossa. Tämä en-
 nalta määrätty muoto voi olla esimerkiksi binaärimuoto, jota on helppo mikroprosessorilla käsitellä. Ensimmäinen merkkijono salataan ensimmäisellä avaimella, jolloin salataan tieto siitä, mitä henkilökohtaisia
 25 tietoja turvamerkinnän muodostamisessa on käytetty. Merkkijono allekirjoitetaan sähköisesti. Tämän jälkeen merkkijono salataan merkintälaitteessa esimerkiksi
 käyttäjän julkisella avaimella salatun merkkijonon muodostamiseksi. Merkintälaitteessa on edullisesti
 kaksi eri salausavainta.

Merkintälaitteessa olevasta käyttäjän julkisesta avaimesta ei ole laitteen ulkopuolella tietoa.
 30 Tällöin identifiointitiedot pysyvät salassa, mikä antaa turvamerkinnän käyttäjälle intimiteettisuoja. Salattu merkkijono tallennetaan sähköisessä muodossa merkintälaitteeseen, joka on liitetty merkittävään
 35 esineeseen tai tuotteeseen.

Turvamerkintä avataan siten, että luetaan salattu merkkijono tunnistuslaitteeseen, joka käsittää

- välineet salatun merkkijonon purkamiseksi. Tunnistuslaitteessa on myös purkuavain, johon vain turvamerkin-
nän omistajalla ja käyttäjällä on käyttöoikeus. Käy-
tännössä käyttöoikeus on purkuavaimen salasana, kuten
5 PIN-koodi, tai muu vastaava koodi, jolla purkuavainta
voi käyttää. Käyttäjä voi lähettää tämän purkuavaimen
myös sellaisessa salatussa muodossa, että luotettava
kolmas osapuoli, esimerkiksi poliisi, voi sen purkaa
ja käyttää tätä avainta turvamerkin-
10 nän tunnistamiseen.
- Edullisesti henkilökohtaisiin tietoihin kuu-
luu turvamerkin-
nän omistajan biometrinen näyte. Bio-
metrinen näyte voi olla DNA-koodi, joka on tallennettu
turvamerkintään ennalta määrättyssä muodossa. Samaten
biometrinen näyte voi olla turvamerkin-
15 nän omistajan
sormenjälkinäyte, silmänpohjan tai iiriksen kuva.
Näistä näytteistä on muodostettu graafinen esitys ja
se on koodattu sopivaan muotoon, esimerkiksi binääri-
muotoon, jotta se voidaan salata käyttäen jotain tun-
nettua salausten menetelmää.
- 20 Kun henkilökohtaisiin tietoihin kuuluu bio-
metrinen näyte, voidaan kaksinkertaisesti varmistaa
se, kenelle turvamerkintä kuuluu. Kun käyttäjä, joka
väittää omistavansa turvamerkin-
nän, antaa salasan-
an, jolla turvamerkintä voidaan purkaa ja saada käyttäjän
25 henkilötiedot, niin ensimmäinen varmistus on suoritettu,
koska purkuavaimen salasana on käyttäjä- ja/tai
henkilökohtainen. Tämän jälkeen käyttäjä voidaan liit-
tää turvamerkintään ottamalla hänestä vastaava näyte
kuin mitä turvamerkintä sisältää. Jos esimerkiksi tur-
30 vamerkin-
nän sisältämä DNA-koodi vastaa käyttäjältä
määritettyä DNA-koodia, voidaan olla täysin varmoja
siitä, että turvamerkintä kuuluu kyseiselle henkilö-
lle.
- Turvamerkintään on liitetty myös omistajan
35 henkilötiedot tunnistusmerkinnän yksilöimiseksi ja
omistajan oikeellisuuden saamiseksi.

Keksinnön mukaiseen järjestelmään turvamerkinnän, jota käytetään esineiden ja laitteiden merkitsemiseen liittämällä turvamerkintä sähköisessä muodossa niihin, käyttämiseksi kuuluu tunnistuslaite, johon
 5 kuuluu lukulaite tunnistusmerkin lukemiseksi ja prosessorin tunnistusmerkin käsittelemiseksi. Tunnistuslaite voi olla mikä tahansa tunnettu laite, jolla sähköisessä muodossa tallennettu turvamerkintä voidaan lukea. Lisäksi tunnistuslaitteen ominaisuudet määräytyvät pitkälti sen perusteella, miten turvamerkintä on
 10 tallennettu. Koska turvamerkintä voidaan tallentaa monessa eri muodossa, kuten graafisessa, viivakoodi-, binääri- tai vastaavassa muodossa, niin voi lukulaitteellakin olla useita ominaisuuksia, vastaavasti.

Keksinnön mukaisesti järjestelmään kuuluu välineet ensimmäisen merkkijonon muodostamiseksi henkilökohtaisista tiedoista ennalta määrättyssä muodossa. Lisäksi järjestelmään kuuluu välineet ensimmäisen merkkijonon salaamiseksi käyttäjän julkisella avaimella
 20 salatun merkkijonon muodostamiseksi. Merkkijonon muodostamisvälineet ja merkkijonon salaamisvälineet voivat olla esimerkiksi tietokoneessa tai muussa vastaavassa laitteessa, johon henkilökohtaiset tiedot syötetään ja jolla turvamerkintä muodostetaan. Lisäksi
 25 järjestelmään kuuluu merkintälaite salatun merkkijonon tallentamiseksi sähköisessä muodossa. Merkintälaitteeseen syötetään salattu merkkijono ennalta määrättyssä muodossa. Edelleen järjestelmään kuuluu välineet salauksen purkamiseksi tunnistuslaitteessa olevalla purku-
 30 avaimella.

Eräässä edullisessa sovelluksessa merkintälaitteeseen kuuluu muistilaite ja ensimmäinen liittytäräjäpinta merkintälaitteen liittämiseksi lukulaitteeseen. Tunnistuslaite voi olla turvamoduuli, johon
 35 kuuluu toinen liityntäräjäpinta yhteyden muodostamiseksi merkintälaitteeseen. Eräässä edullisessa sovel-

luksessa ensimmäinen ja toinen liityntärajapinta on toteutettu Bluetooth-teknologialla.

5 Esillä olevan keksinnön etuna tunnettuun tekniikkaan verrattuna on, että keksintö takaa luotettavan ja turvallisen järjestelyn sähköisessä muodossa olevan turvamerkinnän käyttämiseksi. Lisäksi keksintö merkittävästi yksinkertaistaa sähköisessä muodossa olevan turvamerkinnän käyttöä, koska erillistä rekisteröintitietokantaa ei tarvita.

10 Vielä keksinnön etuna tunnettuun tekniikkaan verrattuna on, että keksinnön ansiosta voidaan turvamerkinnän omistajan oikeellisuus tarkistaa kaksinker-
taisesti. Tällöin usein voidaan täysin varmistua siitä, kenelle turvamerkintä kuuluu. Keksinnön mukainen
15 menettely antaa myös turvamerkinnän käyttäjälle intimitteettisuojan, koska tallennetun turvamerkinnän sisällön selvittäminen on hyvin hankalaa riippuen käytettävästä salausalgoritmista.

20 KUVALUETTELO

Seuraavassa keksintöä selostetaan edullisten sovellusesimerkkien avulla viitaten oheiseen piirustukseen, jossa

25 kuvio 1 esittää erästä esillä olevan keksinnön mukaista tunnistuslaitetta;

kuvio 2 esittää erästä esillä olevan keksinnön mukaista edullista merkintälaitetta; ja

30 kuvio 3 esittää vuokaaviota erästä esillä olevan keksinnön mukaisesta edullista tunnistusmenetelmästä

KEKSINNÖN YKSITYISKOHTAINEN SELOSTUS

35 Kuviossa 1 on esitetty eräs edullinen tunnistuslaite 1. Tunnistuslaitteeseen kuuluu toinen liityntärajapinta RP2 tunnistuslaitteen yhdistämiseksi merkintälaitteeseen 6. Lisäksi tunnistuslaitteeseen kuu-

luu salaus- ja purkuvälineet 5, 7, joilla salataan merkintälaitteeseen 6 tallennettava informaatio ja puretaan merkintälaitteella luettava salattu informaatio.

5 Edelleen kuviossa 1 esitettyihin salausvälineisiin kuuluu prosessori 3, joka voidaan suunnitella ja optimoida erityisesti salaustoimintoja varten ja joka salaa, purkaa salauksen ja toteuttaa sähköisen allekirjoituksen, ja muisti 9, joka on yhdistetty prosessoriin sen tarvitsemien avaimien ja parametrien
10 tallentamiseksi. Muistiin 9 voidaan tallentaa turvamo-
duulin käyttäjän henkilökohtainen purkuavain, käytetyn salausalgoritmin parametrejä ja muita tarpeellisia tietoja. Edullinen esimerkki tässä keksinnössä käytet-
15 tävästä salausalgoritmista on RSA-menetelmä, mutta myös muita epäsymmetrisiä tai symmetrisiä algoritmeja voidaan sovelluksesta riippuen käyttää.

Tunnistuslaitteen runko 11 on sovitettu vastaamaan matkapuhelimen teholahteen muotoja. Lisäksi
20 runkoon 11 on yhdistetty liitin 12, jolla tunnustus-
laite voidaan kytkeä matkapuhelimeen. Liittimen 12 kautta voidaan myös kytkeä teho ja tietoliikenne tunnustuslaitteen ja matkapuhelimen välillä. Tässä sovel-
luksessa tunnustuslaitteen teholähde vastaa kapasiteet-
25 tiltaan olennaisesti matkaviestimen teholähdettä ja on siten myös ladattava. Tällöin tunnustuslaite voidaan helposti mekaanisesti ja sähköisesti kiinnittää matkapuhelimeen.

Kuviossa 2 esitettyyn merkintälaitteeseen
30 kuuluu muistilaite 8 ja ensimmäinen liityntärajapinta RP1 merkintälaitteen yhdistämiseksi ulkoiseen laitteeseen, esimerkiksi tunnustuslaitteeseen. Edullisesti merkintälaite 6 voi olla sinänsä tunnettu transpondere-
ritekniikkaan perustuva yleisesti käytetty merkintä-
35 laite.

Ensimmäisellä ja toisella liityntärajapinnalla RP1, RP2 tunnustuslaite 1 voidaan yhdistää radio-

teitse tai fyysisesti merkintälaitteeseen 6 niiden välistä tiedonsiirtoa varten. Salattu merkkijono voidaan siirtää merkintälaitteeseen 6 tunnistuslaitteella tai merkintälaitteen valmistuksen yhteydessä. Salattu merkkijono voidaan lukea tunnistuslaitteella tai sitä vastaavalla muulla laitteella, jossa on lukemiseen tarvittavat välineet. Eräs tällainen laite voisi olla turvamoduuli, joka kuvataan patenttijulkaisussa FI 981902. Liityntärajapintojen RP1, RP2 yhteyteen voidaan järjestää niin sanottu Bluetooth -osa, vaikka sitä kuvioissa 1 ja 2 ei esitetäkään. Bluetooth -osalla toteutetaan kyseisen teknologian vaatimat toimenpiteet. Liityntärajapinnat RP1, RP2 voidaan toteuttaa millä tahansa optisella infrapunalinkillä, radiolinkillä tai jollakin tunnetulla väyläliitännällä.

Kuviossa 3 esitetään eräs edullinen keksinnön mukainen tunnistusmenetelmä. Kun merkintälaitteella varustettu esine tai laite halutaan tunnistaa, luetaan tunnistuslaitteella 1 merkintälaitteeseen 6 tallennettu informaatio, lohko 31. Lukeminen voi tapahtua radioteitse tai tunnistuslaite voidaan fyysisesti kiinnittää merkintälaitteeseen. Kun informaatio on luettu tunnistuslaitteelle, annetaan tunnistuslaitteeseen käyttäjän henkilökohtainen salasana, joka mahdollistaa tunnistuslaitteella olevan henkilökohtaisen purkuavaimen käytön, lohko 32. Tämä on ensimmäinen tarkistus tarkistettaessa merkintälaitteen omistajaa. Vain merkintälaitteen omistajalla on merkintälaitteelle tallennetun salatun merkkijonon purkamisessa käytettävän purkuavaimen salasana hallussaan.

Kun käyttäjä on antanut avaimen, tallennuslaitteella 1 puretaan salattu merkkijono, lohko 33. Saadusta puretusta merkkijonosta tarkistetaan henkilön identiteetti ja jos se vastaa henkilön ilmoittamaa identiteettiä, jatketaan lohkoon 35 ja jos ei, voidaan lukuoperaatio ja purkuoperaatio toteuttaa uudelleen, esimerkiksi kolme kertaa, jolloin palataan lohkoon 31.

Lohkossa 35, jos vielä halutaan varmistaa, että henkilö on todella se, joka ilmoittaa olevansa, otetaan henkilöstä biometrinen näyte ja verrataan näytettä merkintälaitteelle tallennettuun näyteinformaatioon.

5 Jos näyte on kunnossa, voidaan olla lähes täysin varmoja henkilön identiteetistä ja siitä, että merkintälaite kuuluu kyseiselle henkilölle. Myös tätä näytteen vertailuprosessia voidaan toistaa esimerkiksi kolme kertaa, jos halutaan varmistua siitä, ettei testin

10 epäonnistuminen ole aiheutunut teknisestä viasta.

Keksintö mahdollistaa paikallisesti tapahtuvan luotettavan tunnistuksen ilman, että tunnistamisen yhteydessä täytyy ottaa yhteyttä erilliseen tietokantaan, josta tunnisteiden oikeellisuus tarkistetaan. Eri-

15 tyisesti sähköisen tunnistuksen yleistyessä ajaututaan helposti tilanteeseen, jossa identiteettiä tarkistetaan useista eri tietokannoista, jolloin myös identiteettisuoja voi kärsiä.

Eräässä esimerkinomaisessa tapauksessa muodostetaan käyttäjän henkilökohtaisista tiedoista ensimmäinen merkkijono. Ensimmäiseen merkkijonoon kuuluu esimerkiksi DNA-koodi ja sormenjälkitieto, jotka on muunnettu digitaaliseen muotoon. Näin muodostettu merkkijono salataan RSA 1024-menetelmällä käyttäen

25 käyttäjän salaista salakirjoitusavainta, jolloin muodostetusta merkkijonosta ei voi päätellä, mistä ruumiinosasta tai osista biometrinen tieto koostuu. Merkkijono allekirjoitetaan sähköisesti ja salataan julkisella avaimella. Näin muodostettu tunniste liitetään

30 salattavaan tuotteeseen.

Turvamerkintä voidaan tarkistaa esimerkiksi matkaviestimeen liitettyllä tunnistuslaitteella, jolloin matkaviestimellä voidaan todistaa käyttäjän oikeus merkittyyntä esineeseen tai informaatioon. Sähköinen

35 informaatio voidaan liittää helposti esimerkiksi digitaalisesti tallennettuun tietoon. Esimerkiksi CD-levylle, joka sisältää paljon redundanttista informaatiota.

tiota, voidaan kätkeä vaikeasti havaittava tunniste, joka löytyy vasta sopivan funktion ulostulona. Informaatioon sekoitettua turvamerkintää ei voi muuttaa, koska se ei näy ulospäin. Turvamerkintä voidaan lukea
5 esimerkiksi jollain tarkistuslukumenetelmällä, jolloin informaation ulostulona saadaan haluttu turvamerkintä. Näin voidaan varmentaa esimerkiksi sähköisen informaation tekijänoikeustietoja, toisin sanoen merkitä sähköinen informaatio jonkin henkilön tai yhteisön
10 nimiin.

Esillä olevaa keksintöä eri rajata edellä esitettyihin esimerkkeihin, vaan monet muunnokset ovat mahdollisia pysyttäessä oheisten patenttivaatimuksien suojapiirissä.

PATENTTIVAATIMUKSET

1. Menetelmä turvamerkinnän tunnistamiseksi,
jossa menetelmässä turvamerkintää käytetään esineiden,
laitteiden tai informaation merkitsemiseen liittämällä
5 turvamerkintä sähköisessä muodossa niihin, tun-
nettu siitä, että

luetaan turvamerkintä tunnistuslaitteeseen;
ja

avataan turvamerkintä sen sisältämien henki-
10 lökohtaisten tietojen saamiseksi.

2. Patenttivaatimuksen 1 mukainen menetelmä,
tunnettu siitä, että turvamerkintä muodostetaan siten,
että

muodostetaan henkilökohtaisista tiedoista en-
15 simmäinen merkkijono ennalta määrättyssä muodossa;

salataan ensimmäinen merkkijono;

allekirjoitetaan ensimmäinen merkkijono säh-
köisesti;

salataan allekirjoitettu ensimmäinen merkki-
20 jono salatun merkkijonon muodostamiseksi;

tallennetaan salattu merkkijono sähköisessä
muodossa merkintälaitteeseen; ja että turvamerkintä
avataan siten, että

luetaan salattu merkkijono tunnistuslaittee-
25 seen; ja

puretaan salaus tunnistuslaitteessa olevalla
purkuavaimella.

3. Patenttivaatimuksen 1 tai 2 mukainen mene-
telmä, tunnettu siitä, että henkilökohtaisiin
30 tietoihin kuuluu turvamerkinnän omistajan biometrinen
näyte.

4. Jonkin patenttivaatimuksista 1 - 3 mukai-
nen menetelmä, tunnettu siitä, että biometriseen
näytteeseen kuuluu turvamerkinnän omistajan DNA-koodi
35 ennalta määrättyssä muodossa.

5. Jonkin patenttivaatimuksista 1 - 3 mukai-
nen menetelmä, tunnettu siitä, että biometriseen

näytteeseen kuuluu turvamerkin­nän omistajan sormenjälkinäyte ennalta määrätyssä muodossa.

5 6. Jonkin patenttivaatimuksista 1 - 3 mukainen menetelmä, tunnettu siitä, että biometriseen näytteeseen kuuluu kuva turvamerkin­nän omistajan silmästä ennalta määrätyssä muodossa.

7. Jonkin patenttivaatimuksista 1 - 6 mukainen menetelmä, tunnettu siitä, että biometrinen näyte on binäärimuodossa.

10 8. Jonkin patenttivaatimuksista 1 - 7 mukainen menetelmä, tunnettu siitä, että liitetään turvamerkintään sen omistajan henkilötiedot turvamerkin­nän yksilöimiseksi.

15 9. Järjestelmä turvamerkin­nän, jota käytetään esineiden ja laitteiden merkitsemiseen liittämällä turvamerkintä sähköisessä muodossa niihin, käyttämiseksi, johon järjestelmään kuuluu tunnistuslaite (1), johon kuuluu lukulaite (2) turvamerkin­nän lukemiseksi ja prosessori (3) turvamerkin­nän käsittelemiseksi,

20 tunnettu siitä, että järjestelmään kuuluu välineet (4) ensimmäisen merkkijonon muodostamiseksi henkilökohtaisista tiedoista ennalta määrätyssä muodossa;

25 välineet (5) ensimmäisen merkkijonon salaamiseksi käyttäjän julkisella avaimella salatun merkkijonon muodostamiseksi;

merkintälaite (6) salatun merkkijonon tallentamiseksi sähköisessä muodossa;

30 välineet (7) salauksen purkamiseksi tunnistuslaitteessa olevalla purkuavaimella.

10. Patenttivaatimuksen 9 mukainen järjestelmä, tunnettu siitä, että merkintälaitteeseen (6) kuuluu muistilaite (8) ja ensimmäinen liitäntärajapinta (RP1) merkintälaitteen liittämiseksi lukulaitteeseen (2).

35

11. Patenttivaatimuksen 9 tai 10 mukainen järjestelmä, tunnettu siitä, että tunnistuslaite (1) on turvamoduuli.

5 12. Jonkin edeltävistä patenttivaatimuksista 9 - 11 mukainen järjestelmä, tunnettu siitä, että turvamoduuliin (1) kuuluu toinen liityntärajapinta (RP2) yhteyden muodostamiseksi merkintälaitteeseen.

(57) TIIVISTELMÄ

Esillä olevan keksinnön kohteena on menetelmä ja järjestelmä merkintälaitteen tunnistamiseksi. Keksinnössä käytetään hyväksi informaation salausta ja henkilöstä otettavaa biometristä näytettä. Tämä menetelmä mahdollistaa merkintälaitteen tehokkaan ja luotettavan tunnistamisen. Käytännössä menetelmällä ja järjestelmällä saadaan kaksinkertainen varmistus merkintälaitteen omistajan oikeellisuudesta. Ensin varmistetaan sillä, että omistajan on tiedettävä merkintälaitteelle tallennetun informaation salaukseen käytettävän avaimen salasana ja toiseksi vielä sillä, että henkilöstä otettavan biometrisen näytteen on vastattava merkintälaitteelle tallennettua biometristä näytteen koodia tai siitä muodostettua informaatiota.

(Fig. 1)

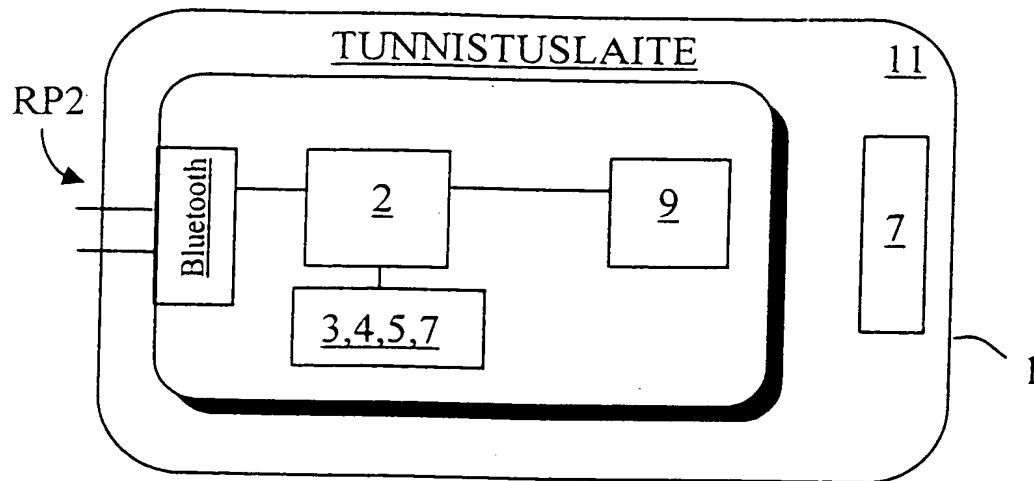


Fig. 1

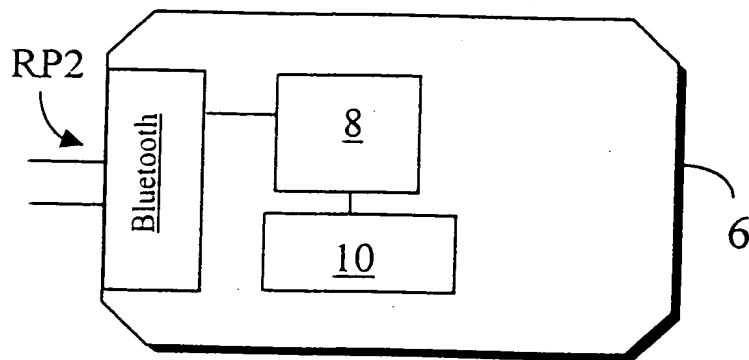


Fig. 2

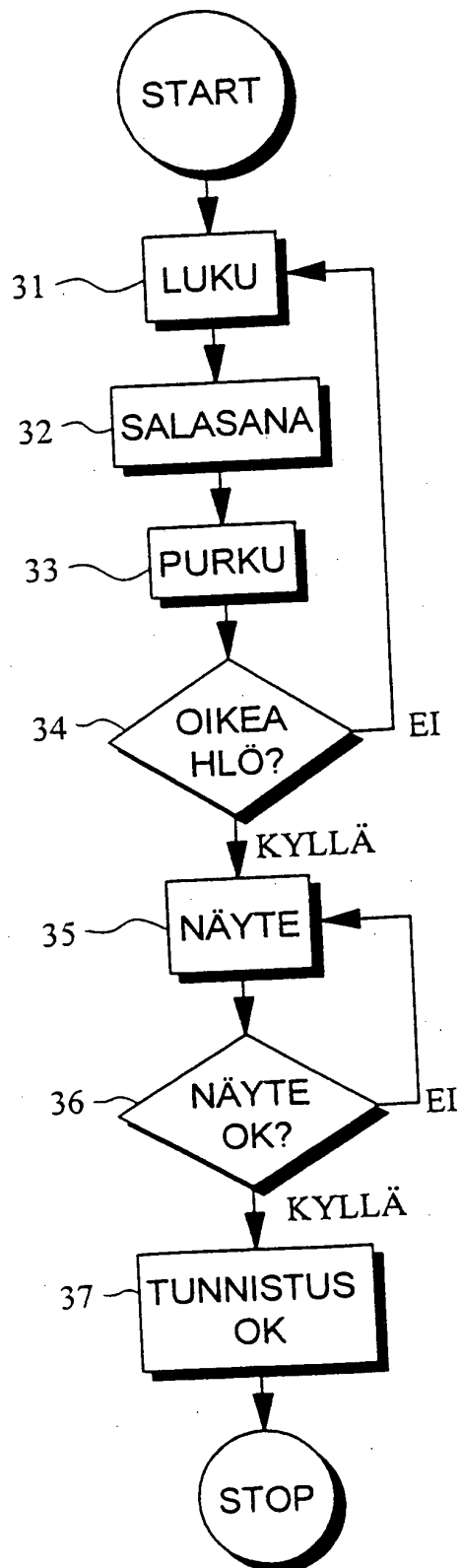


Fig 3